日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: １９９９年　９月２１日

出 願 番 号
Application Number: 平成１１年特許願第２６６８５３号

出 願 人
Applicant (s): カシオ計算機株式会社

２０００年　２月２５日

特 許 庁 長 官
Commissioner,
Patent Office 近 藤 隆

出証番号　出証特２０００－３００９９７８

【書類名】　特許願

【整理番号】　99-0598-00

【あて先】　特許庁長官殿

【国際特許分類】　G06F 17/00

G06F 13/00

【発明者】

【住所又は居所】　東京都羽村市栄町３丁目２番１号

カシオ計算機株式会社羽村技術センター内

【氏名】　大塚　基

【特許出願人】

【識別番号】　000001443

【氏名又は名称】　カシオ計算機株式会社

【代理人】

【識別番号】　100074985

【弁理士】

【氏名又は名称】　杉村　次郎

【手数料の表示】

【予納台帳番号】　023180

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9109737

【プルーフの要否】　要

【書類名】　　明細書

【発明の名称】セキュリティ管理システムおよびそのプログラム記録媒体

【特許請求の範囲】

【請求項１】

サーバ装置側で管理しているアプリケーションソフト／データを持ち運び自在な記録媒体を介して端末装置側に外部供給するコンピュータシステムにおいて、

前記サーバ装置は、接続された端末装置から固有の端末識別情報を読み込む読込手段と、

この読込手段によって読み込まれた固有の端末識別情報の他、アプリケーションソフト／データと共にその管理情報を記録媒体に書き込む書込手段と、

前記アプリケーションソフト／データの管理情報をスクランブル処理して暗号化するスクランブル処理手段とを具備し、

前記端末装置は、アプリケーションソフト／データが格納されている記録媒体がセットされている状態で、この記録媒体内のアプリケーションソフト／データをアクセスする際に、当該記録媒体から端末識別情報を読み出して自己の端末識別情報と比較する比較手段と、

この比較手段によって各端末識別情報の一致が検出された際に、前記スクランブル処理されているアプリケーションソフト／データの管理情報を復元するスクランブル復元手段とを具備したことを特徴とするセキュリティ管理システム。

【請求項２】

前記サーバ装置は、前記読込手段によって端末装置から読み込んだ固有の端末識別情報を暗号化する暗号化手段を有し、前記書込手段は前記暗号化手段によって暗号化された端末識別情報を記録媒体に書き込み、

前記端末装置は、アプリケーションソフト／データおよび暗号化された端末識別情報が格納されている記録媒体がセットされている状態で、この記録媒体内のアプリケーションソフト／データをアクセスする際に、当該記録媒体から暗号化された端末識別情報を読み出してそれを復元する暗号復元手段を有し、前記比較手段は前記暗号復元手段によって復元された端末識別情報と自己の端末識別情報とを比較するようにしたことを特徴とする請求項１記載のセキュリティ管理シス

テム。

【請求項３】

前記サーバ装置は、前記スクランブル処理手段によって前記アプリケーションソフト／データの管理情報をスクランブル処理した際に使用したスクランブル処理用の暗号キーを端末装置に書き込む書込手段を有し、

前記スクランブル復元手段は、前記スクランブル処理用の暗号キーを用いてアプリケーションソフト／データの管理情報を復元するようにしたことを特徴とする請求項１記載のセキュリティ管理システム。

【請求項４】

サーバ装置側で管理しているアプリケーションソフト／データを持ち運び自在な記録媒体を介して各端末装置側に外部供給するコンピュータシステムにおいて、

前記サーバ装置は、接続された端末装置から固有の端末識別情報を読み込む読込手段と、

この読込手段によって読み込んだ固有の端末識別情報を暗号化する暗号化手段と、

この暗号化手段によって暗号化された固有の端末識別情報の他、アプリケーションソフト／データを記録媒体に書き込む書込手段とを具備し、

前記端末装置は、アプリケーションソフト／データおよび暗号化された端末識別情報が格納されている記録媒体が端末装置にセットされている状態で、この記録媒体内のアプリケーションソフト／データをアクセスする際に、当該記録媒体から暗号化された端末識別情報を読み出してそれを復元する暗号復元手段と、

この暗号復元手段によって復元された端末識別情報と自己の端末識別情報とを比較する比較手段と、

この比較手段によって各端末識別情報の一致が検出された際に、その記録媒体内のアプリケーションソフト／データに対するアクセスを許可するアクセス制御手段とを具備したことを特徴とするセキュリティ管理システム。

【請求項５】

前記暗号化手段によって暗号化された固有の端末識別情報と共に、アプリケー

ションソフトを記録媒体に書き込む際に、前記書込手段はアプリケーションソフトに対応付けてそのアクセス制御用のプログラムとこのアクセス制御用プログラム内に前記暗号化された固有の端末識別情報を組み込み、

前記端末装置は、アプリケーションソフト内に前記アクセス制御用プログラムおよび端末識別情報が組み込まれている記録媒体がセットされた場合に、この記録媒体内のアクセス制御用プログラムを起動させると共に、このアクセス制御用プログラムにしたがって前記暗号化端末識別情報を読み出してそれを復元すると共に、復元された端末識別情報と当該端末装置から読み出した端末識別情報とを比較し、この結果、各端末識別情報の一致が検出された場合には、記録媒体内の対応するアプリケーションソフトのアクセスを許可し、各端末識別情報の不一致が検出された場合には、そのアプリケーションソフトのアクセスを禁止するようにしたことを特徴とする請求項４記載のセキュリティ管理システム。

【請求項６】

前記サーバ装置は、同一グループに属する複数台の端末装置を識別するグループ識別情報と前記読込手段によって読み込んだ固有の端末識別情報とに基づいてそのグループ固有のグループ端末識別情報を生成する生成手段を有し、

前記書込手段は前記生成手段によって生成されたグループ端末識別情報を記録媒体と端末装置にそれぞれ書き込み、

前記端末装置は、アプリケーションソフト／データおよびグループ端末識別情報が格納されている記録媒体がセットされている状態で、この記録媒体内のアプリケーションソフト／データをアクセスする際に、前記比較手段は、サーバ装置から当該端末装置に書き込まれたグループ端末識別情報と当該記録媒体から読み出されたグループ端末識別情報とを比較するようにしたことを特徴とする請求項１あるいは４記載のセキュリティ管理システム。

【請求項７】

前記サーバ装置は、前記暗号化手段によって端末識別情報を暗号化した際に使用した端末識別情報用の暗号キーを端末装置に書き込む書込手段を有し、

前記端末装置は、アプリケーションソフト／データおよび暗号化された端末識別情報が格納されている記録媒体がセットされている状態で、この記録媒体内の

アプリケーションソフト／データをアクセスする際に、前記暗号復元手段は前記端末識別情報用の暗号キーを用いて当該記録媒体内の暗号化端末識別情報を復元するようにしたことを特徴とする請求項２あるいは４記載のセキュリティ管理システム。

【請求項８】

コンピュータが読み取り可能なプログラムコードを有する記録媒体であって、

接続された端末装置から固有の端末識別情報を読み込ませるコンピュータが読み取り可能なプログラムコードと、

読み込まれた固有の端末識別情報の他、アプリケーションソフト／データと共にその管理情報を記録媒体に書き込ませるコンピュータが読み取り可能なプログラムコードと、

前記アプリケーションソフト／データの管理情報をスクランブル処理させるコンピュータが読み取り可能なプログラムコードと、

アプリケーションソフト／データが格納されている記録媒体が端末装置にセットされている状態でこの記録媒体内のアプリケーションソフト／データをアクセスする際に、当該記録媒体から端末識別情報を読み出して自己の端末識別情報と比較させるコンピュータが読み取り可能なプログラムコードと、

この結果、各端末識別情報の一致が検出された際に、前記スクランブル処理されているアプリケーションソフト／データの管理情報を復元させるコンピュータが読み取り可能なプログラムコードとを有する記録媒体。

【請求項９】

コンピュータが読み取り可能なプログラムコードを有する記録媒体であって、

接続された端末装置から固有の端末識別情報を読み込ませるコンピュータが読み取り可能なプログラムコードと、

端末装置から読み込んだ固有の端末識別情報を暗号化させるコンピュータが読み取り可能なプログラムコードと、

暗号化された固有の端末識別情報の他、アプリケーションソフト／データを記録媒体に書き込ませるコンピュータが読み取り可能なプログラムコードと、

アプリケーションソフト／データおよび暗号化された端末識別情報が格納され

ている記録媒体が端末装置にセットされている状態でこの記録媒体内のアプリケーションソフト／データをアクセスする際に、当該記録媒体から暗号化された端末識別情報を読み出してそれを復元させるコンピュータが読み取り可能なプログラムコードと、

復元された端末識別情報と自己の端末識別情報とを比較させるコンピュータが読み取り可能なプログラムコードと、

各端末識別情報の一致が検出された際に、その記録媒体内のアプリケーションソフト／データに対するアクセスを許可させるコンピュータが読み取り可能なプログラムコードとを有する記録媒体。

【請求項１０】

コンピュータが読み取り可能なプログラムコードを有する記録媒体であって、

接続された端末装置から固有の端末識別情報を読み込ませるコンピュータが読み取り可能なプログラムコードと、

読み込まれた固有の端末識別情報の他、アプリケーションソフト／データと共にその管理情報を記録媒体に書き込ませるコンピュータが読み取り可能なプログラムコードと、

前記記録媒体に書き込まれたアプリケーションソフト／データの管理情報をスクランブル処理させるコンピュータが読み取り可能なプログラムコードとを有する記録媒体。

【請求項１１】

コンピュータが読み取り可能なプログラムコードを有する記録媒体であって、

アプリケーションソフト／データが格納されている記録媒体が端末装置にセットされている状態でこの記録媒体内のアプリケーションソフト／データをアクセスする際に、当該記録媒体から端末識別情報を読み出して自己の端末識別情報と比較させるコンピュータが読み取り可能なプログラムコードと、

この結果、各端末識別情報の一致が検出された際に、前記スクランブル処理されているアプリケーションソフト／データの管理情報を復元させるコンピュータが読み取り可能なプログラムコードとを有する記録媒体。

【請求項１２】

コンピュータが読み取り可能なプログラムコードを有する記録媒体であって、

接続された端末装置から固有の端末識別情報を読み込ませるコンピュータが読み取り可能なプログラムコードと、

端末装置から読み込んだ固有の端末識別情報を暗号化させるコンピュータが読み取り可能なプログラムコードと、

暗号化された固有の端末識別情報の他、アプリケーションソフト／データを記録媒体に書き込ませるコンピュータが読み取り可能なプログラムコードとを有する記録媒体。

【請求項１３】

コンピュータが読み取り可能なプログラムコードを有する記録媒体であって、

アプリケーションソフト／データおよび暗号化された端末識別情報が格納されている記録媒体が端末装置にセットされている状態でこの記録媒体内のアプリケーションソフト／データをアクセスする際に、当該記録媒体から暗号化された端末識別情報を読み出してそれを復元させるコンピュータが読み取り可能なプログラムコードと、

復元された端末識別情報と自己の端末識別情報とを比較させるコンピュータが読み取り可能なプログラムコードと、

各端末識別情報の一致が検出された際に、その記録媒体内のアプリケーションソフト／データに対するアクセスを許可させるコンピュータが読み取り可能なプログラムコードとを有する記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

この発明は、サーバ側のアプリケーションソフト／データを持ち運び自在な記録媒体を介して端末側に外部供給するコンピュータシステムにおいて、記録媒体内のアプリケーションソフト／データに対する安全性を保障するセキュリティ管理システムおよびそのプログラム記録媒体に関する。

【０００２】

【従来の技術】

一般に、アプリケーションソフトはフロッピーディスクやコンパクトディスク等の記録媒体を介してパーソナルコンピュータに別途提供され、これをインストールすることにより起動される。この場合、ソフトメーカはアプリケーションソフトにユニークなプロダクト番号を付けて出荷する。このソフトをユーザがパソコン上でインストールして動作させる場合、許可キーとしてこのプロダクト番号をキーボードから入力するようにしている。

一方、複数台の端末装置がネットワークを介して通信接続されてなるオンライン型のクライアント・サーバシステムにおいて、各クライアント端末はネットワークを介してアプリケーションソフトを入手するようにしている。

【０００３】

【発明が解決しようとする課題】

しかしながら、記録媒体を介して提供されるアプリケーションソフトは、そのプロダクト番号さえ分かれば、複数台のパソコンに何回でもインストールすることができ、不法なコピー複製が可能となる。このようなコピー複製を禁止するためには、一旦、アプリケーションソフトをインストールしたらその記録媒体の内容を全てクリアする必要がある。しかしながら、記録媒体内の内容を全てクリアしてしまうと、その後、障害が発生し、再度インストールする必要が生じた時には、それに対応することができなくなり、まは、記録媒体の内容をその都度クリアするという面倒な作業を強要することにもなる。

また、ネツトワーク経由でクライアント端末からサーバーへアクセスする場合、ユーザＩＤとパスワードとを知っていれば、誰でもどの端末からでもアプリケーションソフトをアクセスすることができ、不正なアクセスの可能性がある。

こととことはアプリケーションソフトに限らず、企業情報などの機密性の高い重要データが格納されている記録媒体を介して端末装置に提供する場合であっても同様であり、この記録媒体を誤って紛失してしまうと第３者に重要データを見られてしまい、セキュリティ維持の点で問題があった。

第１の発明の課題は、サーバ装置側で管理しているアプリケーションソフト／データを持ち運び自在な記録媒体を介して端末装置側に外部提供する場合、記録媒体と端末装置との対応付けを端末識別情報の一致、不一致およびアプリケーシ

ョンソフト／データを管理する管理情報の暗号化、複合化によって行うことで、特定の端末装置に対してのみアプリケーションソフト／データのアクセスを許可できるようにすることである。

第２の発明の課題は、サーバ装置側で管理しているアプリケーションソフト／データを持ち運び自在な記録媒体を介して端末装置側に外部提供する場合、記録媒体と端末装置との対応付けを端末識別情報の暗号化、複合化によって行うことで、特定の端末装置に対してのみアプリケーションソフト／データのアクセスを許可できるようにすることである。

【０００４】

この発明の手段は、次の通りである。

請求項第１記載の発明（第１の発明）は、サーバ装置側で管理しているアプリケーションソフト／データを持ち運び自在な記録媒体を介して端末装置側に外部供給するコンピュータシステムにおいて、前記サーバ装置は、接続された端末装置から固有の端末識別情報を読み込む読込手段と、この読込手段によって読み込まれた固有の端末識別情報の他、アプリケーションソフト／データと共にその管理情報を記録媒体に書き込む書込手段と、前記アプリケーションソフト／データの管理情報をスクランブル処理して暗号化するスクランブル処理手段とを具備し、前記端末装置は、アプリケーションソフト／データが格納されている記録媒体がセットされている状態で、この記録媒体内のアプリケーションソフト／データをアクセスする際に、当該記録媒体から端末識別情報を読み出して自己の端末識別情報と比較する比較手段と、この比較手段によって各端末識別情報の一致が検出された際に、前記スクランブル処理されているアプリケーションソフト／データの管理情報を復元するスクランブル復元手段とを具備するものである。

なお、この発明は次のようなものであってもよい。

（１）前記サーバ装置は、前記読込手段によって端末装置から読み込んだ固有の端末識別情報を暗号化する暗号化手段を有し、前記書込手段は前記暗号化手段によって暗号化された端末識別情報を記録媒体に書き込み、前記端末装置は、アプリケーションソフト／データおよび暗号化された端末識別情報が格納されている記録媒体がセットされている状態でこの記録媒体内のアプリケーションソフト

／データをアクセスする際に、当該記録媒体から暗号化された端末識別情報を読み出してそれを復元する暗号復元手段を有し、前記比較手段は前記暗号復元手段によって復元された端末識別情報と自己の端末識別情報とを比較する。

この場合、前記サーバ装置は、前記暗号化手段によって端末識別情報を暗号化した際に使用した端末識別情報用の暗号キーを端末装置に書き込む書込手段を有し、前記端末装置は、アプリケーションソフト／データおよび暗号化された端末識別情報が格納されている記録媒体がセットされている状態でこの記録媒体内のアプリケーションソフト／データをアクセスする際に、前記暗号復元手段は前記端末識別情報用の暗号キーを用いて当該記録媒体内の暗号化端末識別情報を復元する。

（２）前記サーバ装置は、前記スクランブル処理手段によって前記アプリケーションソフト／データの管理情報をスクランブル処理した際に使用したスクランブル処理用の暗号キーを端末装置に書き込む書込手段を有し、前記スクランブル復元手段は、前記スクランブル処理用の暗号キーを用いてアプリケーションソフト／データの管理情報を復元する。

（３）前記サーバ装置は、同一グループに属する複数台の端末装置を識別するグループ識別情報と前記読込手段によって読み込んだ固有の端末識別情報とに基づいてそのグループ固有のグループ端末識別情報を生成する生成手段を有し、前記書込手段は前記生成手段によって生成されたグループ端末識別情報を記録媒体と端末装置にそれぞれ書き込み、前記端末装置は、アプリケーションソフト／データおよびグループ端末識別情報が格納されている記録媒体がセットされている状態でこの記録媒体内のアプリケーションソフト／データをアクセスする際に、前記比較手段は、サーバ装置から当該端末装置に書き込まれたグループ端末識別情報と当該記録媒体から読み出されたグループ端末識別情報とを比較する。

請求項１記載の発明においては、サーバ装置は、接続された端末装置から固有の端末識別情報を読み込むと共に、読み込んだ固有の端末識別情報の他、アプリケーションソフト／データとその管理情報を記録媒体に書き込む。そして、前記アプリケーションソフト／データの管理情報をスクランブル処理して暗号化する。前記端末装置は、アプリケーションソフト／データが格納されている記録媒体

がセットされている状態でこの記録媒体内のアプリケーションソフト／データをアクセスする際に、当該記録媒体から端末識別情報を読み出して自己の端末識別情報と比較し、その結果、各端末識別情報の一致が検出された際に、前記スクランブル処理されているアプリケーションソフト／データの管理情報を復元する

したがって、サーバ装置側で管理しているアプリケーションソフト／データを持ち運び自在な記録媒体を介して端末装置側に外部提供する場合、記録媒体と端末装置との対応付けを端末識別情報の一致、不一致およびアプリケーションソフト／データを管理する管理情報の暗号化、複合化によって行うことで、特定の端末装置に対してのみアプリケーションソフト／データのアクセスを許可することができる。

【０００５】

請求項第２記載の発明（第２の発明）は、サーバ装置側で管理しているアプリケーションソフト／データを持ち運び自在な記録媒体を介して各端末装置側に外部供給するコンピュータシステムにおいて、前記サーバ装置は、接続された端末装置から固有の端末識別情報を読み込む読込手段と、この読込手段によって読み込んだ固有の端末識別情報を暗号化する暗号化手段と、この暗号化手段によって暗号化された固有の端末識別情報の他、アプリケーションソフト／データを記録媒体に書き込む書込手段とを具備し、前記端末装置は、アプリケーションソフト／データおよび暗号化された端末識別情報が格納されている記録媒体が端末装置にセットされている状態でこの記録媒体内のアプリケーションソフト／データをアクセスする際に、当該記録媒体から暗号化された端末識別情報を読み出してそれを復元する暗号復元手段と、この暗号復元手段によって復元された端末識別情報と自己の端末識別情報とを比較する比較手段と、この比較手段によって各端末識別情報の一致が検出された際に、その記録媒体内のアプリケーションソフト／データに対するアクセスを許可するアクセス制御手段とを具備するものである。なお、この発明は次のようなものであってもよい。

（１）前記暗号化手段によって暗号化された固有の端末識別情報と共に、アプリケーションソフトを記録媒体に書き込む際に、前記書込手段はアプリケーションソフトに対応付けてそのアクセス制御用のプログラムとこのアクセス制御用プ

ログラム内に前記暗号化された固有の端末識別情報を組み込み、前記端末装置は、アプリケーションソフト内に前記アクセス制御用プログラムおよび端末識別情報が組み込まれている記録媒体がセットされた場合、この記録媒体内のアクセス制御用プログラムを起動させると共に、このアクセス制御用プログラムにしたがって前記暗号化端末識別情報を読み出してそれを復元すると共に、復元された端末識別情報と当該端末装置から読み出した端末識別情報とを比較し、この結果、各端末識別情報の一致が検出された場合には、記録媒体内の対応するアプリケーションソフトのアクセスを許可し、各端末識別情報の不一致が検出された場合には、そのアプリケーションソフトのアクセスを禁止する。

（２）前記サーバ装置は、同一グループに属する複数台の端末装置を識別するグループ識別情報と前記読込手段によって読み込んだ固有の端末識別情報とに基づいてそのグループ固有のグループ端末識別情報を生成する生成手段を有し、前記書込手段は前記生成手段によって生成されたグループ端末識別情報を記録媒体に書き込み、前記端末装置は、アプリケーションソフト／データおよびグループ端末識別情報が格納されている記録媒体がセットされている状態でこの記録媒体内のアプリケーションソフト／データをアクセスする際に、前記比較手段は、サーバ装置から当該端末装置に書き込まれたグループ端末識別情報と当該記録媒体から読み出されたグループ端末識別情報とを比較する。

（３）前記サーバ装置は、前記暗号化手段によって端末識別情報を暗号化した際に使用した端末識別情報用の暗号キーを端末装置に書き込む書込手段を有し、前記端末装置は、アプリケーションソフト／データおよび暗号化された端末識別情報が格納されている記録媒体がセットされている状態でこの記録媒体内のアプリケーションソフト／データをアクセスする際に、前記暗号復元手段は前記端末識別情報用の暗号キーを用いて当該記録媒体内の暗号化端末識別情報を復元する。

請求項２記載の発明においては、サーバ装置は、接続された端末装置から固有の端末識別情報を読み込むと共に、それを暗号化する。そして、暗号化した固有の端末識別情報の他、アプリケーションソフト／データを記録媒体に書き込む。端末装置は、アプリケーションソフト／データおよび暗号化された端末識別情報

が格納されている記録媒体が端末装置にセットされている状態でこの記録媒体内のアプリケーションソフト／データをアクセスする際に、当該記録媒体から暗号化された端末識別情報を読み出してそれを復元すると共に、復元された端末識別情報と自己の端末識別情報とを比較し、この結果、各端末識別情報の一致が検出された際に、その記録媒体内のアプリケーションソフト／データに対するアクセスを許可する。

したがって、サーバ装置側で管理しているアプリケーションソフト／データを持ち運び自在な記録媒体を介して端末装置側に外部提供する場合、記録媒体と端末装置との対応付けを端末識別情報の暗号化、複合化によって行うことで、特定の端末装置に対してのみアプリケーションソフト／データのアクセスを許可することができる。

【０００６】

【発明の実施の形態】

（第１実施形態）

以下、図１～図７を参照してこの発明の第１実施形態を説明する。

図１は、この実施形態におけるセキュリティ管理システムの全体構成を示したブロック図である。

このセキュリティ管理システムは、サーバ装置側で記憶管理されているアプリケーションソフト／データを持ち運び自在な記録媒体を介して端末装置側に外部提供するもので、この記録媒体内のアプリケーションソフト／データに対してセキュリティ維持を図り、第三者による複製コピー等を防止するようにしている。すなわち、このシステムは、例えば、会社組織において会社側に設置させているサーバ装置１と、各営業担当者が持参するモバイル型のクライアント端末（携帯端末装置）２とを有し、各営業担当者は外出先で可搬型記録媒体３内のアプリケーションソフト／データをアクセスしながら営業活動を行い、そして、1日の営業終了時に端末本体から可搬型記録媒体３を抜き取り、それをサーバ装置１側のカードライタ４にセツトすると、サーバ装置１はカードライタ４を介して記録媒体３内の営業記録を収集処理するようにしている。そして、サーバ装置１と複数台の携帯端末装置２とはシリアルケーブル５を介して着脱自在に接続可能となっ

ている。すなわち、サーバ装置１と複数台の携帯端末装置２とは必要に応じて接続することができるようになっている。

【０００７】

可搬型記録媒体３は例えば、コンパクトフラッシュカードによって構成されているもので、以下、コンパクトフラッシュカードをＣＦカードと称する。ここで、図中、各ＣＦカードに付した「＃Ａ」「＃Ｂ」、「＃Ｃ」、‥‥は、端末名称「Ａ」、「Ｂ」、「Ｃ」、‥‥で示される携帯端末装置２に対応付けられた端末対応のカードであることを示している。なお、この実施形態においては端末対応のカードの他、後述する端末グループ対応のカードも存在するが、図１の例では端末対応のカードのみを示している。カードライタ４はＣＦカード３を複数枚同時にセット可能なもので、複数のカード挿入口を有している。

そして、サーバ装置１はＣＦカード３を介して携帯端末装置２側にアプリケーションソフト／データベースファイル（以下ＡＰソフト／データと称する）を配布する。すなわち、サーバ装置１はＣＦカード３に書き込む書込対象、つまり、配布対象のＡＰソフト／データが任意に指定された際に、ＡＰソフト／データベース格納部６をアクセスしてそれに対応するＡＰソフト／データを呼び出してカードライタ４に与え、それにセットされている１または２以上のＣＦカード３にＡＰソフト／データを書き込む。

【０００８】

その際、ＣＦカード３に格納したＡＰソフト／データの管理情報、つまり、ＦＡＴ（Ｆｉｌｅ・Ａｌｌｏｃａｔｉｏｎ・Ｔａｂｌｅ）およびルートディレクトリの領域を指定してその内容をスクランブル処理（暗号化処理）するが、この場合、スクランブル処理用として任意に生成された暗号キーを用いてスクランブルが行われる。なお、スクランブル処理（暗号化処理）をどのような手法で行うかは、任意であり、任意に生成された暗号キーを用いてＡＰソフト／データの管理情報を暗号化するようにしている。また、各携帯端末装置２には予め設定されている固有の端末識別情報（製造番号）が記憶されており、サーバ装置１は各携帯端末装置２から固有の端末識別情報（製造番号）を読み込むと、任意に生成された暗号キーを用いて端末識別情報を暗号化し、ＣＦカード３に書き込む。そして

、この端末識別情報の暗号化に使用された暗号キーとスクランブル処理時に使用された暗号キーは、携帯端末装置２に書き込まれる。

【０００９】

携帯端末装置２は、ＡＰソフト／データが格納されているＣＦカード３がカードライタ７にセットされている状態で、このＣＦカード３内のＡＰソフト／データをアクセスする際に、このカードから暗号化端末識別情報を読み出すと共に、サーバ装置１から自己のメモリに書き込まれている端末識別情報用の暗号キーを読み出し、この暗号キーを用いて暗号化端末識別情報を復元する。そして、自己メモリに予め設定されている端末識別情報を呼び出し、復元した端末識別情報と自己の設定端末識別情報とを比較する。この結果、各端末識別情報の一致が検出された際に、スクランブル処理されているＡＰソフト／データの管理情報を復元する。その際、スクランブル処理用の暗号キーを読み出してＡＰソフト／データのＦＡＴおよびルーブディレクトリを復元することにより、ＡＰソフト／データに対するアクセスを許可するようにしている。

【００１０】

図2は、ＣＦカード３の内容を示した図で、サーバ装置１によってＣＦカード３には「スクランブルフラグ」、「暗号化識別情報」、「ＦＡＴ」、「ルートディレクトリ」、「ＡＰソフト／データ」が書き込まれる。ここで、「スクランブルフラグ」は、ＣＦカード３内に格納されているＡＰソフト／データの「ＦＡＴ」、「ルートディレクトリ」がスクランブル処理されている状態にあることを示すフラグであり、また「暗号化識別情報」は携帯端末装置２から読み込んだ固有の端末識別情報（製造番号）がサーバ装置１によって暗号化されたものである。「ＦＡＴ」、「ルートディレクトリ」は配布対象としての１または2以上のＡＰソフト／データを管理する管理情報であり、その内容はスクランブル処理されている。

【００１１】

図3は、例えば、グループ「営業１課」、「営業２課」‥‥のように端末グループ対応のＣＦカード３を示した図で、図中、「＃Ａ１」、「＃Ａ２」、「＃Ａ３」で示す各ＣＦカード３は、端末名称が「Ａ１」、「Ａ２」、「Ａ３」である各

携帯端末装置２が属する端末グループＡ対応の記録媒体であり、同様に、「＃Ｂ１」、「＃Ｂ２」‥‥で示す各ＣＦカード３は、端末名称が「Ｂ１」、「Ｂ２」、‥‥である各携帯端末装置２が属する端末グループＢ対応の記録媒体であり、同一グループ内の各ＣＦカード３はそのグループに属する各携帯端末装置２で共通して使用することができるようになっている。この端末グループ対応のＣＦカード３内にはグループ端末識別情報が書き込まれる。このグループ端末識別情報はそのグループに属する１台目の携帯端末装置２から読み込んだ固有の端末識別情報（製造番号）と、任意に入力したグループ名との組み合わせによって生成されたもので、同一グループの各ＣＦカード３には、同一のグループ端末識別情報が書き込まれる。

【００１２】

図４は、サーバ装置１／各端末装置２の全体構成を示したブロック図であり、それらは基本的に同様の構成となっているため、同一符号を付して示す。

ＣＰＵ１１は、記憶装置１２内のオペレーティングシステムや各種アプリケーションソフトにしたがってこのサーバ装置１や端末装置２の全体動作を制御する中央演算処理装置である。記憶装置１２は、オペレーティングシステムや各種アプリケーションソフトの他、データベース、文字フォント等が格納され、磁気的、光学的、半導体メモリ等によって構成されている記録媒体１３やその駆動系を有している。この記録媒体１３はハードディスク等の固定的な媒体若しくは着脱自在に装着可能なＣＤ－ＲＯＭ、フロッピィデスク、ＲＡＭカード、磁気カード等の可搬型の媒体である。また、この記録媒体１３内のプログラムやデータは、必要に応じてＣＰＵ１１の制御によりＲＡＭ（例えば、スタティクＲＡＭ）１４にロードされたり、ＲＡＭ１４内のデータが記録媒体１３にセーブされる。更に、記録媒体はサーバ等の外部機器側に設けられているものであってもよく、ＣＰＵ11は伝送媒体を介してこの記録媒体内のプログラム／データを直接アクセスして使用することもできる。

また、ＣＰＵ１１は記録媒体３内に格納されるその一部あるいは全部を他の機器側から伝送媒体を介して取り込み、記録媒体１３に新規登録あるいは追加登録することもできる。すなわち、コンピュータ通信システムを構成する他の機器（

例えば、サーバ・ホスト・クライアントコンピュータ）から通信回線やケーブル等の有線伝送路あるいは電波、マイクロウエーブ、赤外線等の無線伝送路を介して送信されてきたプログラム／データを伝送制御部１５によって受信して記録媒体１３内にインストールすることができる。更に、プログラム／データはサーバ等の外部機器側で記憶管理されているものであってもよく、ＣＰＵ１１は伝送媒体を介して外部機器側のプログラム／データを直接アクセスして使用することもできる。

【００１３】

このようにＣＰＵ11は、予め固定的に常駐されているプログラム／データに限らず、記録媒体や伝送媒体を介して外部供給されたプログラム／データを利用して、あるいは外部機器側で記憶管理されているプログラム／データを直接利用してこの実施形態特有の動作を実行することもできる。一方、ＣＰＵ１１にはその入出力周辺デバイスである伝送制御部１５、入力部１６、表示部１７、印字部１８、カードリーダ／ライタ１９がバスラインを介して接続されており、入出力プログラムにしたがってＣＰＵ１１はそれらの動作を制御する。伝送制御部１５は、例えば、通信モデムや赤外線モジュールあるいはアンテナ等を含む通信インターフェイスである。入力部１６はキーボードやタッチパネルあるいはマウスやタッチ入力ペン等のポインティングデバイスを構成する操作部であり、文字列データや各種コマンドを入力する。なお、表示部１７は、フルカラー表示を行う液晶やＣＲＴあるいはプラズマ表示装置などであり、印字部１８は熱転写やインクジェットなどのノンインパクトプリンタあるいはドットインパクトプリンタである。カードリーダ／ライタ１９はＣＦカード３に対してその書き込み／読み込み動作を行う。

【００１４】

次に、この第１実施形態におけるサーバ装置１、携帯端末装置２の動作を図５～図７に示すフローチャートを参照して説明する。ここで、これらのフローチャートに記述されている各機能を実現するためのプログラムは、読み取り可能なプログラムコードの形態で記録媒体１３に格納されており、ＣＰＵ１１はこのプログラムコードにしたがった動作を逐次実行する。また、ＣＰＵ１１は伝送媒体を

介して伝送されてきた上述のプログラムコードにしたがった動作を逐次実行することもできる。このことは、後述する他の実施形態においても同様であり、記録媒体の他、伝送媒体を介して外部供給されたプログラム／データを利用してこの実施形態特有の動作を実行することもできる。

【００１５】

図５および図6は、サーバ装置１に携帯端末装置２、ＣＦカード３が接続されている状態で、サーバ装置１側で記憶管理されているＡＰソフト／データを持ち運び自在なＣＦカード３を介して端末装置２側に外部提供する場合におけるサーバ装置１側の動作を示したフローチャートである。

先ず、ユーザは書き込み対象のＡＰソフト／データを全て選択すると（ステップＡ１）、ＣＰＵ１１はＡＰソフト／データベース格納部６から選択指定されたＡＰソフト／データおよびそのＦＡＴ、ルートディレクトリを取得しておく（ステップＡ２）。また、ユーザは書き込み対象の端末を指定すると（ステップＡ３）、その指定内容に応じて指定端末のみの書き込みか、グループ対応書き込みかを調べる（ステップＡ４）。いま、指定端末のみの書き込みが指定された場合には、指定端末から「製造番号」を読み出すと共に（ステップＡ５）、それを暗号化するための暗号キーを生成する（ステップＡ６）。この場合、暗号キーはランダムに生成した数値データ等であり、指定端末から読み出した「製造番号」をこの暗号キーを用いて暗号化し、端末識別情報を生成する（ステップＡ７）。

【００１６】

そして、スクランブル処理用の暗号キーを生成するが（ステップＡ８）、この暗号キーもランダムに生成した数値データ等である。このようにして生成した端末識別情報暗号用の暗号キーと、スクランブル処理用の暗号キーとを指定端末に書き込む（ステップＡ９）。また、指定端末対応のＣＦカード３には、ステップＡ２で取得したＡＰソフト／データとそのＦＡＴ、ルートディレクトリおよびステップＡ７で暗号化した端末識別情報を書き込む（ステップＡ１０）。そして、ＣＦカード３に書き込んだＡＰソフト／データのＦＡＴとルートディレクトリをステップＡ８で生成した暗号キーを用いてスクランブル処理して暗号化すると共に（ステップＡ１１）、そのＣＦカード３内の「スクランブルフラグ」をＯＮす

る（ステップＡ１２）。これによって指定端末に対する処理が終わると、ステップＡ１３でそのことが検出されてこのフローの終了となる。

【００１７】

一方、グループ対応の書き込みが指定された場合には（ステップＡ４）、図6のフローチャートに進み、先ず、そのグループ端末識別情報を生成する処理が行われる。すなわち、上述したようにグループ端末識別情報は、そのグループに属する１台目の携帯端末装置２から読み込んだ固有の端末識別情報（製造番号）と、任意に入力したグループ名との組み合わせによって生成するようにしているため、グループ内の１台目の端末であれば（ステップＡ１５）、そのグループ識別情報（グループ名）を任意に入力すると（ステップＡ１６）、その１台目の端末から端末識別情報（製造番号）を読み出し（ステップＡ１７）、このグループ名と製造番号とに基づいてそのグループ固有のグループ端末識別情報を生成する（ステップＡ１８）。例えば、グループ名が「営業１課」、製造番号が「Ｃ０００１」であれば、グループ端末識別情報として「Ｃ０００１営業１課」が生成される。

そして、このグループ端末識別情報を暗号化するための暗号キーをランダム生成すると共に（ステップＡ１９）、この生成キーを用いてグループ端末識別情報を暗号化する（ステップＡ２０）。また、スクランブル処理用の暗号キーを生成しておく（ステップＡ２１）。次に、グループ端末識別情報と共に、その暗号化キーおよびスクランブル処理用の暗号キーを指定端末、この場合、１台目の携帯端末装置２に書き込む（ステップＡ２２）。

【００１８】

そして、図５のステップＡ１０に戻り、指定端末対応のＣＦカード３に、ＡＰソフト／データとそのＦＡＴ、ルートディレクトリ、暗号化グループ端末識別情報を書き込む。そして、そのＦＡＴ、ルートディレクトリをスクランブル処理用の暗号キーを用いてスクランブル処理すると共に（ステップＡ１１）、スクランブルフラグをＯＮさせる（ステップＡ１２）。このような処理は指定グループ内の全端末に対して実行される。すなわち、ステップＡ１３では指定グループ内の全端末終了かを調べ、終了していなければ、ステップＡ１４に進み、同一グルー

プ内の次の端末を指定したのち、図６のステップＡ１５に進み、グループ端末識別情報と共に、その暗号化キーおよびスクランブル処理用の暗号キーを指定端末、この場合、２台目の携帯端末装置２に書き込む。以下、指定グループ内の全端末終了まで上述の動作を繰り返すことにより、同一グループの各携帯端末装置２には同一の内容が書き込まれると共に、そのグループの書く携帯端末装置２およびＣＦカード３には、同一のグループ端末識別情報が書き込まれる。

【００１９】

図７は、各携帯端末装置２側での動作を示したフローチャートであり、ＣＦカード３へのアクセスが指定された際に、このフローチャートにしたがった動作が実行開始される。

先ず、ＣＰＵ１１はＣＦカード３がセットされているかを調べ（ステップＢ１）、セットされていなければ、通常処理のメインフローに戻るが、セットされていれば、そのＣＦカード３から端末識別情報を読み出すと共に（ステップＢ２）、サーバ装置１から自己の端末に書き込まれた端末情報暗号用の暗号キーを読み出し（ステップＢ３）、この端末識別情報を暗号キーに基づいて複合化する（ステップＢ４）。そして、予め自己の設定情報である端末識別情報を読み出し（ステップＢ５）、複合化した端末識別情報と比較し（ステップＢ６）、両者が一致するかを調べる（ステップＢ７）。

【００２０】

ここで、不一致が検出された場合には、当該カードに対するアクセスを不可として処理終了となるが、両者の一致が検出された場合には、ＣＦカード３内のスクランブルフラグはＯＮされているかを調べる（ステップＢ８）。ここで、スクランブルフラグがＯＮされていなければ、端末識別情報の一致のみを条件としてＣＦカード３に対するアクセスを許可するが、スクランブルフラグがＯＮされていれば、サーバ装置１から自己の端末に書き込まれたスクランブル処理用の暗号キーを読み出し（ステップＢ９）、ＣＦカード３内のＦＡＴ、ルートディレクトリをこの暗号キーに基づいて複合化する（ステップＢ１０）。これによってＣＦカード３へのアクセスが可能となる。

【００２１】

以上のように、この第１実施形態おいて、サーバ装置１は、接続された携帯端末装置２から固有の端末識別情報を読み込むと共に、読み込んだ固有の端末識別情報の他、ＡＰソフト／データとそのＦＡＴ、ルートディレクトリをＣＦカード３に書き込み、更に、ＣＦカード３内のＦＡＴ、ルートディレクトリをクランブル処理して暗号化する。一方、携帯端末装置２は、ＡＰソフト／データが格納されているＣＦカード３がセットされている状態において、このＣＦカード３内のＡＰソフト／データをアクセスする際に、当該ＣＦカード３から暗号化された端末識別情報を読み出してそれを復元し、自己の端末識別情報と比較した結果、それらの一致が検出された際に、スクランブル処理されているＡＰソフト／データのＦＡＴ、ルートディレクトリを復元するようにしたから、そのＣＦカード３に対するアクセスを許可することができる。すなわち、サーバ装置１側で管理しているＡＰソフト／データを持ち運び自在なＣＦカード３を介して携帯端末装置２側に外部提供する場合、ＣＦカード３と携帯端末装置２との対応付けを端末識別情報の一致、不一致およびＡＰソフト／データのＦＡＴ、ルートディレクトリの暗号化、複合化によって行うことで、特定の端末に対してのみＡＰソフト／データのアクセスを許可することができ、端末毎のアクセス制御によってアクセス権限を有しない他の端末による不法なコピー複製を効果的に禁止することができるようになる。この場合、端末識別情報およびＡＰソフト／データのＦＡＴ、ルートディレクトリを暗号化するようにしたから、安全性はきわめて高くなる。

このことは、端末対応のカードに限らず、グループ対応のカードについても同様であり、例えば、営業地域毎に特定のＡＰソフト／データを使用する場合、地域毎に端末グループを分けておけば、地域毎のアクセス制御が可能となる。

【００２２】

（第２実施形態）

以下、この発明の第２実施形態について図８～図１０を参照して説明する。なお、上述した第１実施形態は、ＣＦカード３毎のアクセス制御を示したが、この第２実施形態はＣＦカード３内に書き込まれているＡＰソフト毎にアクセス制御を行うようにしたものである。そして、ＡＰソフトのＦＡＴ、ルートディレクトリに対するスクランブル処理は行わず、また、ＡＰソフト内にそのアクセスを制

御する制御プログラムと暗号化された端末識別情報を組み込むようにしている。ここで、両実施形態において基本的に同一のものは、同一符号を付して示し、その説明を省略する他、以下、第2実施形態の特徴部分を中心に説明するものとする。

【００２３】

図８、図９は、上述した第１実施形態で示した図５、図６に対応する動作を示したフローチャートである。

先ず、書き込み対象のＡＰソフトを１つ選択すると（ステップＣ１）、選択指定されたＡＰソフトを取得し（ステップＣ２）、また、書き込み対象の端末を指定すると（ステップＣ３）、その指定内容に応じて指定端末のみの書き込みか、グループ対応書き込みかを調べ（ステップＣ４）、指定端末のみの書き込みが指定された場合には、指定端末から「製造番号」を読み出す（ステップＣ５）。そして、それを暗号化するための暗号キーを生成し（ステップＣ６）、指定端末から読み出した「製造番号」をこの暗号キーで暗号化し、端末識別情報を生成する（ステップＣ７）。次に、暗号キーを指定端末に書き込むと共に（ステップＣ８）、指定端末対応のＣＦカード３にＡＰソフトを書き込む（ステップＣ９）。そして、このＣＦカード３内にそのＡＰソフトに対応付けてアクセス制御用プログラムを組み込むと共に（ステップＣ１０）、このアクセス制御用プログラム内に暗号化端末識別情報を埋め込む（ステップＣ１１）。これによって指定端末に対する処理が終わると、ステップＣ１２でそのことが検出されてこのフローの終了となる。

【００２４】

一方、グループ対応の書き込みが指定された場合には（ステップＣ４）、図９のフローチャートに進み、先ず、上述した第１実施形態と同様に、そのグループ端末識別情報を生成する処理が行われる（ステップＣ１５～Ｃ１８）。そして、このグループ端末識別情報を暗号化するための暗号キーをランダム生成すると共に（ステップＣ１９）、この生成キーを用いてグループ端末識別情報を暗号化する（ステップＣ２０）。次に、グループ端末識別情報と共に、その暗号化キーを指定端末に書き込む（ステップＣ２１）。そして、図８のステップＣ９に戻り、

指定端末対応のＣＦカード３に、ＡＰソフト／データを書き込む。そして、このＣＦカード３内にそのＡＰソフトに対応付けてアクセス制御用プログラムを組み込むと共に（ステップＣ１０）、このアクセス制御用プログラム内に暗号化端末識別情報を埋め込む（ステップＣ１１）。このような処理は指定グループ内の全端末に対して実行される。すなわち、ステップＣ１２では指定グループ内の全端末終了かを調べ、終了していなければ、ステップＣ１３に進み、同一グループ内の次の端末を指定したのち、図９のステップＣ１５に進み、グループ端末識別情報と共に、その暗号化キーを指定端末に書き込む。以下、指定グループ内の全端末終了まで上述の動作を繰り返す。

【００２５】

図１０は、上述した第１実施形態で示した図７に対応する動作を示したフローチャートである。

先ず、ＣＦカード３がセットされていなければ（ステップＤ１）、通常処理のメインフローに戻るが、セットされていれば、そのＣＦカード３内のＡＰソフト対応のアクセス制御用プログラムを起動させる（ステップＤ２）。そして、このアクセス制御用プログラムにしたがってＣＦカード３から端末識別情報を読み出すと共に（ステップＤ３）、サーバ装置１から自己の端末に書き込まれた端末情報暗号用の暗号キーを読み出し（ステップＤ４）、この端末識別情報を暗号キーに基づいて複合化する（ステップＤ５）。そして、予め自己の設定情報である端末識別情報を読み出し（ステップＤ６）、複合化した端末識別情報と比較し（ステップＤ７）、両者が一致するかを調べる（ステップＤ８）。ここで、不一致が検出された場合には、当該カードに対するアクセスを不可として処理終了となるが（ステップＤ９）、両者の一致が検出された場合には、それに対応するＡＰソフトを起動可能としてそのアクセスを許可する（ステップＤ１０）。

【００２６】

以上のように、この第２実施形態おいては、サーバ装置１側で管理しているＡＰソフト／データを持ち運び自在なＣＦカード３を介して携帯端末装置２側に外部提供する場合、ＣＦカード３と携帯端末装置２との対応付けを端末識別情報の暗号化、複合化によって行うことで、特定の端末に対してのみＡＰソフトのアク

セスを許可することができる。この場合、ＣＦカード３内にそのＡＰソフト毎にアクセス制御用プログラムを組み込むと共に、このアクセス制御用プログラム内に暗号化端末識別情報を埋め込むようにしたから、このアクセス制御用プログラムにしたがってＡＰソフト毎のアクセス制御が可能となる。

【００２７】

なお、上述した各実施形態においては、持ち運び自在な記録媒体としてＣＦカード３を例示したが、これに限らず、磁気的、光学的記録媒体等、任意であり、また、クライアント端末はモバイル型の端末に限らず、デスクトップ型の端末であってもよい。また、グループ端末識別情報は、そのグループに属する１台目の携帯端末装置２から読み込んだ固有の製造番号と、任意に入力したグループ名との組み合わせによって生成するようにしたが、１台目の携帯端末装置２から読み込んだ製造番号に限らず、その作成は任意であり、ユニークなグループ端末識別情報であればよい。

【００２８】

【発明の効果】

第１の発明によれば、サーバ装置側で管理しているアプリケーションソフト／データを持ち運び自在な記録媒体を介して端末装置側に外部提供する場合、記録媒体と端末装置との対応付けを端末識別情報の一致、不一致およびアプリケーションソフト／データを管理する管理情報の暗号化、複合化によって行うようにしたから、特定の端末装置に対してのみアプリケーションソフト／データのアクセスを許可することができ、セキュリティ維持と共に、アクセス権限を有しない他の装置による不法なコピー複製を効果的に禁止することが可能となる。

第２の発明によれば、サーバ装置側で管理しているアプリケーションソフト／データを持ち運び自在な記録媒体を介して端末装置側に外部提供する場合、記録媒体と端末装置との対応付けを端末識別情報の暗号化、複合化によって行うようにしたから、特定の端末装置に対してのみアプリケーションソフト／データのアクセスを許可することができ、セキュリティ維持と共に、アクセス権限を有しない他の装置による不法なコピー複製を効果的に禁止することが可能となる。特に、記録媒体内において、アプリケーションソフト毎にアクセス制御用プログラム

を組み込むと共に、このアクセス制御用プログラム内に暗号化端末識別情報を埋め込むようにすれば、このアクセス制御用プログラムにしたがってアプリケーションソフト毎のアクセス制御が可能となる。

【図面の簡単な説明】

【図１】

セキュリティ管理システムの全体構成を示したブロック図。

【図２】

ＣＦカード３の内容を示した図。

【図３】

端末グループ対応のＣＦカード３を示した図。

【図４】

サーバ装置１／各端末装置２の全体構成を示したブロック図。

【図５】

サーバ装置１側で記憶管理されているＡＰソフト／データを持ち運び自在なＣＦカード３を介して端末装置２側に外部提供する場合におけるサーバ装置１側の動作を示したフローチャート。

【図６】

図５に続くサーバ装置１側の動作を示したフローチャート。

【図７】

ＣＦカード３へのアクセスが指定された際に実行開始される各携帯端末装置２側での動作を示したフローチャート。

【図８】

第２実施形態において、サーバ装置１側で記憶管理されているＡＰソフトを持ち運び自在なＣＦカード３を介して端末装置２側に外部提供する場合におけるサーバ装置１側の動作を示したフローチャート。

【図９】

図８に続くサーバ装置１側の動作を示したフローチャート。

【図１０】

第２実施形態において、ＣＦカード３へのアクセスが指定された際に実行開始

される各携帯端末装置２側での動作を示したフローチャート。

【符号の説明】

１　サーバ装置１

２　携帯端末装置２

３　ＣＦカード３

４　カードライタ４

６　ＡＰソフト／データベース格納部６

７　カードライタ７

１１　ＣＰＵ

１２　記憶装置

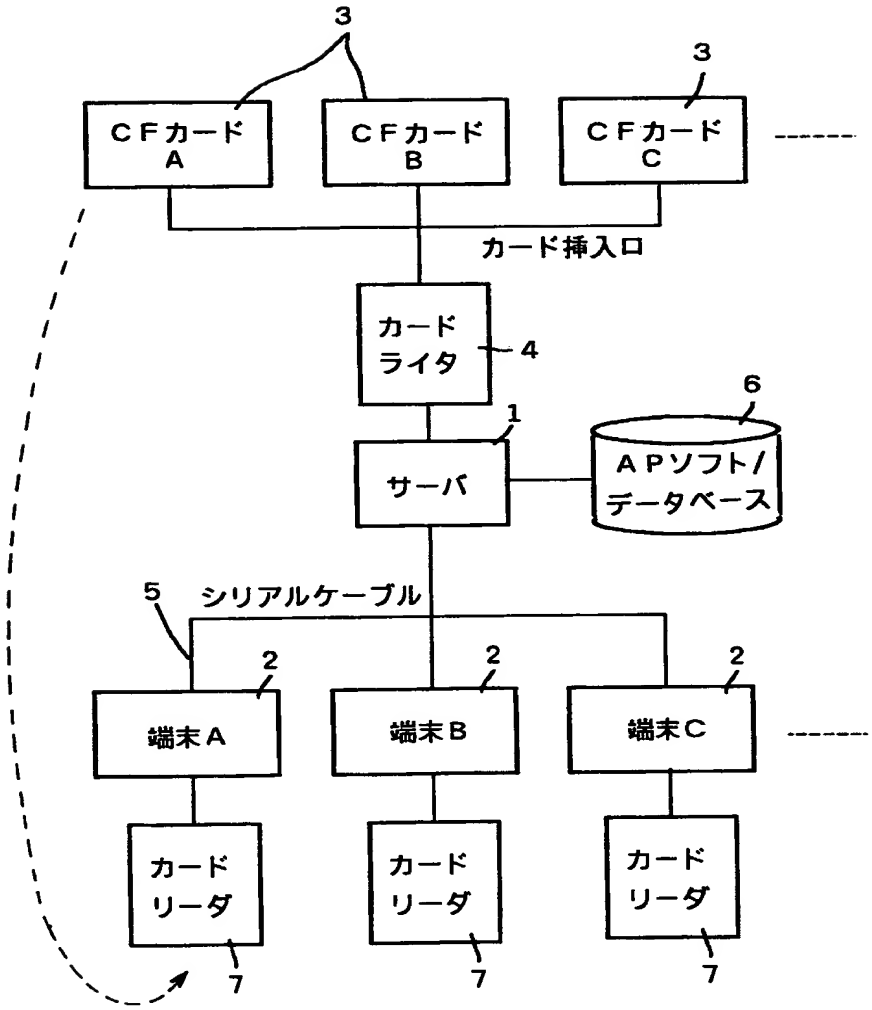
１３　記録媒体

１５　伝送制御部

１６　入力部

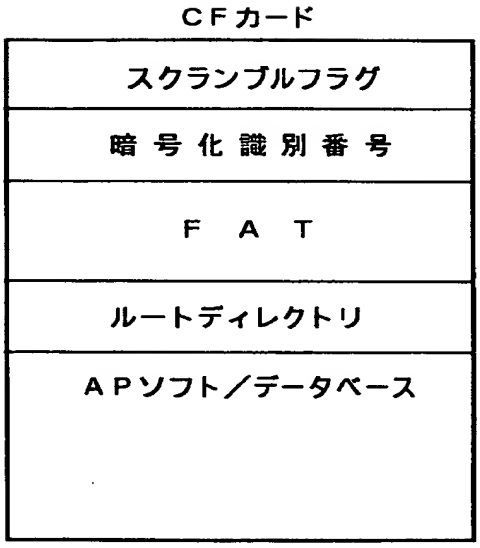
【書類名】　　図面

【図１】

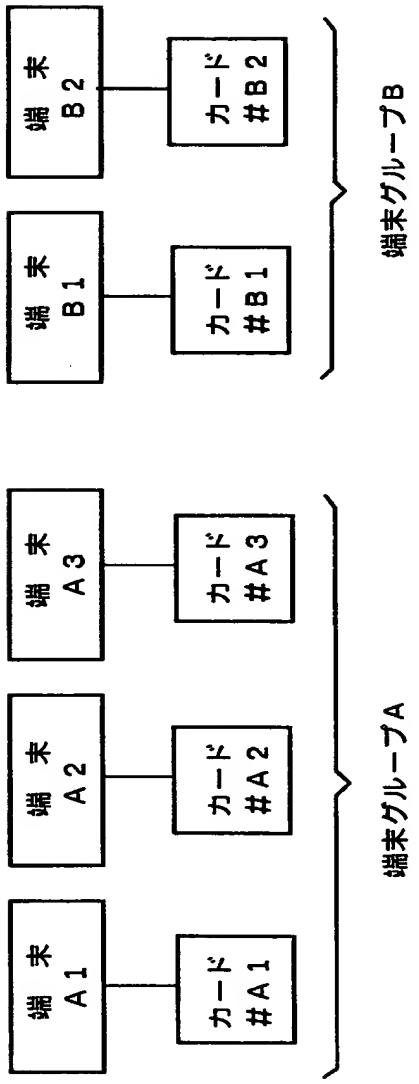


出証特２０００－３００９９７８

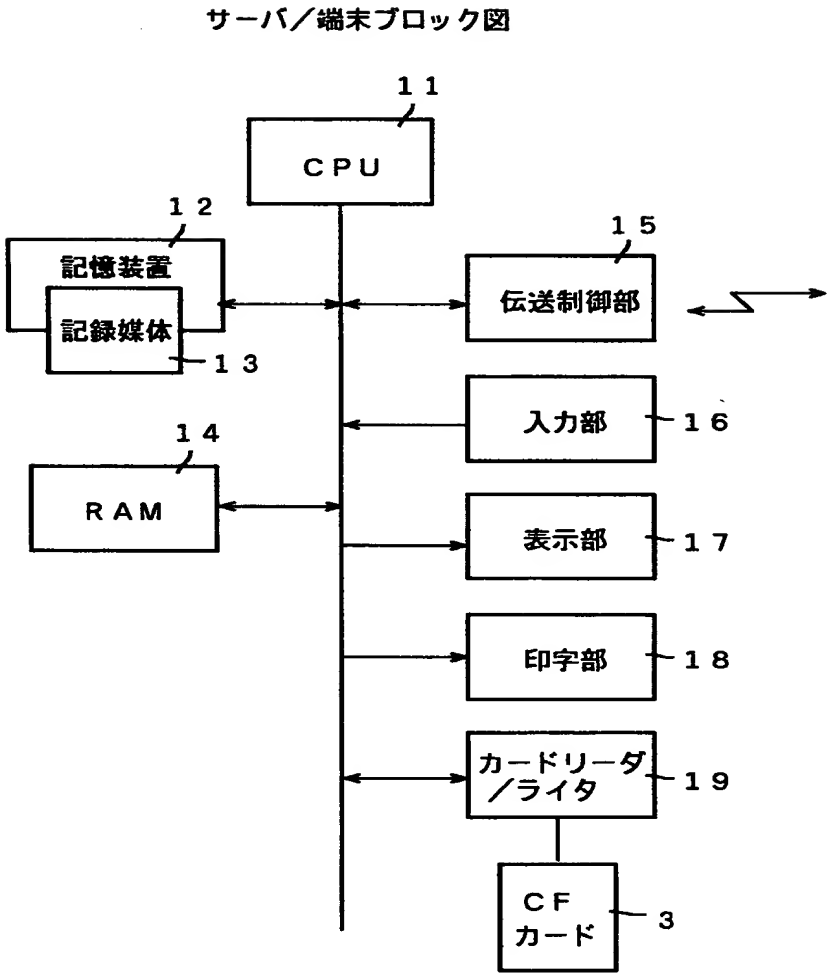
【図２】



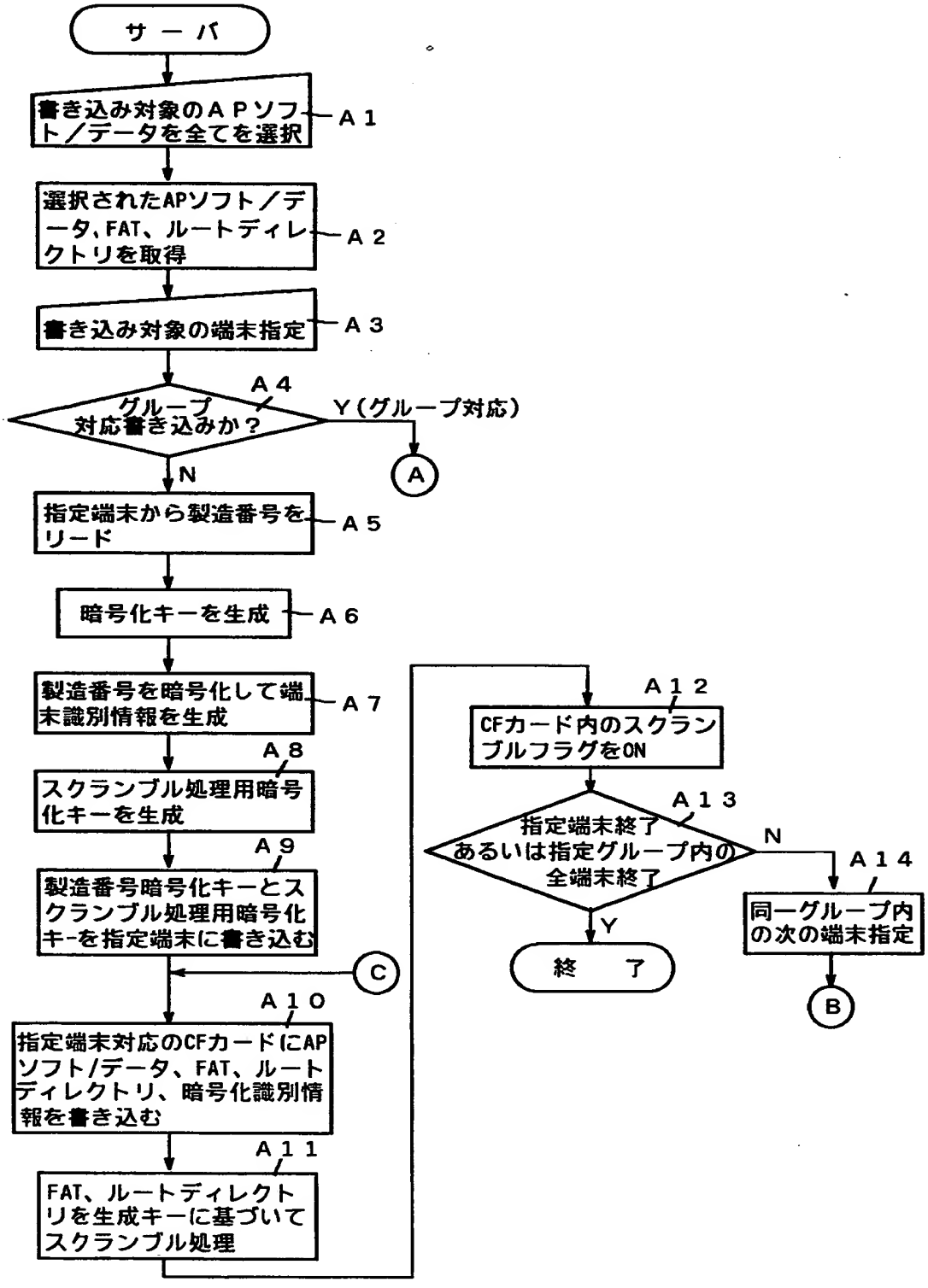
【図３】


端末
A1
カード
#A1
端末
A2
カード
#A2
端末
A3
カード
#A3
端末グループA
端末
B1
カード
#B1
端末
B2
カード
#B2
端末グループB

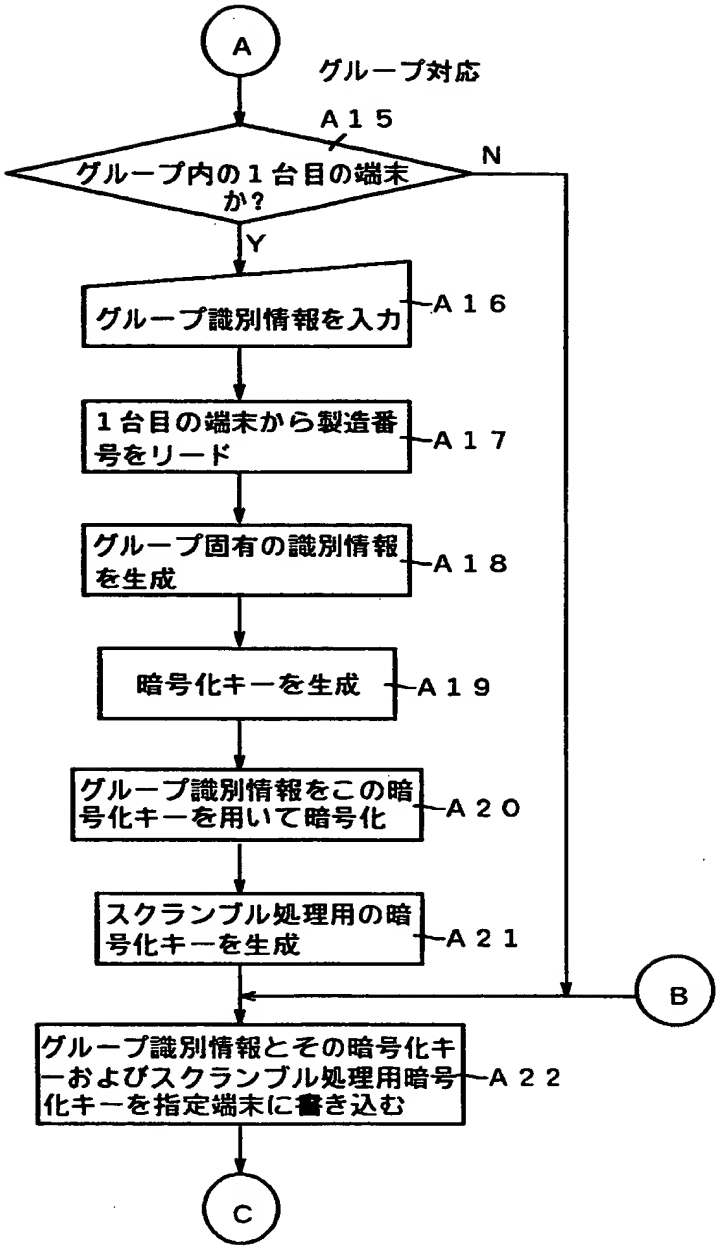
【図４】


サーバ／端末ブロック図
１１
CPU
１２
記憶装置
記録媒体
１３
１４
RAM
１５
伝送制御部
入力部
１６
表示部
１７
印字部
１８
カードリーダ／ライタ
１９
CF カード
３

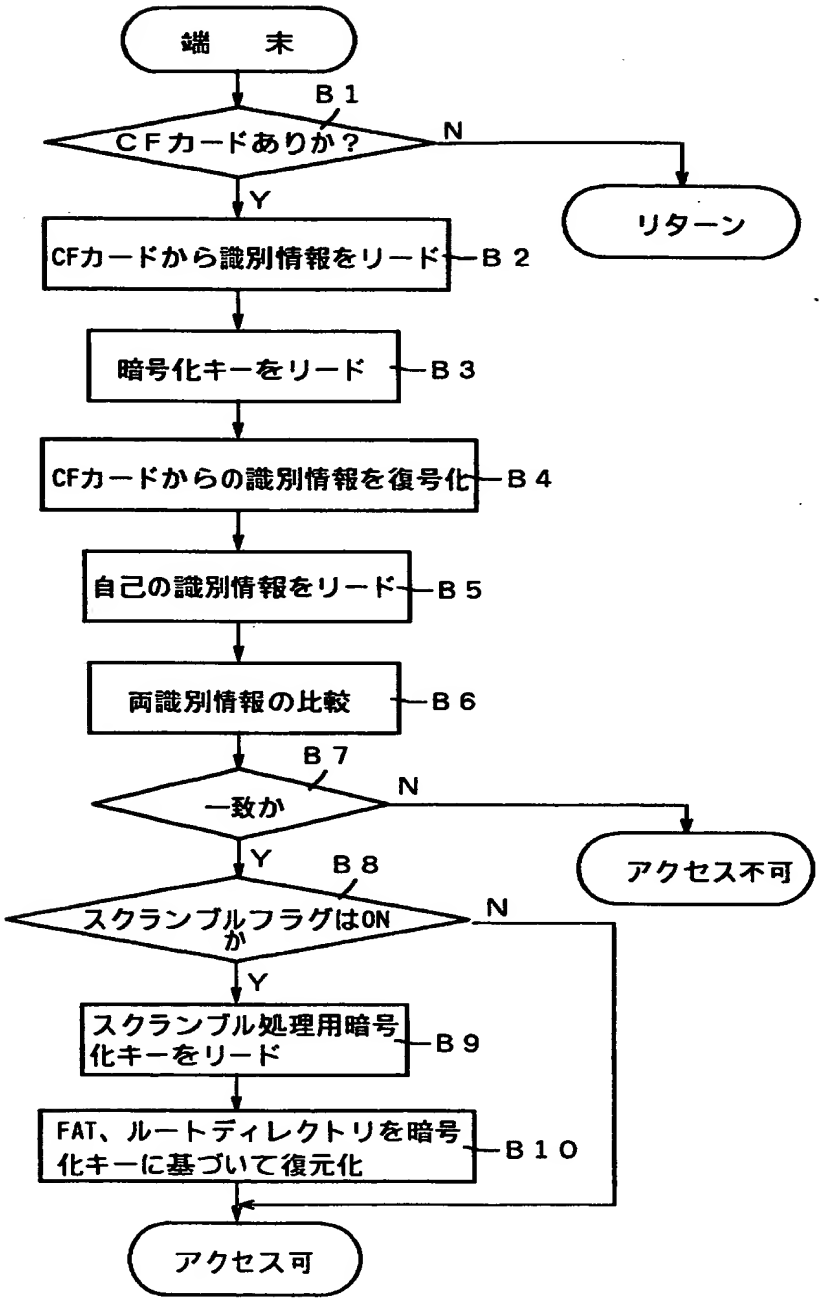
【図５】


サーバ
書き込み対象のＡＰソフト／データを全てを選択
Ａ１
選択されたAPソフト／データ、FAT、ルートディレクトリを取得
Ａ２
書き込み対象の端末指定
Ａ３
Ａ４
グループ対応書き込みか？
Ｙ（グループ対応）
Ａ
Ｎ
指定端末から製造番号をリード
Ａ５
暗号化キーを生成
Ａ６
製造番号を暗号化して端末識別情報を生成
Ａ７
Ａ８
スクランブル処理用暗号化キーを生成
Ａ９
製造番号暗号化キーとスクランブル処理用暗号化キーを指定端末に書き込む
Ｃ
Ａ１０
指定端末対応のCFカードにAPソフト/データ、FAT、ルートディレクトリ、暗号化識別情報を書き込む
Ａ１１
FAT、ルートディレクトリを生成キーに基づいてスクランブル処理
Ａ１２
CFカード内のスクランブルフラグをON
Ａ１３
指定端末終了あるいは指定グループ内の全端末終了
Ｎ
Ａ１４
同一グループ内の次の端末指定
Ｂ
Ｙ
終　了

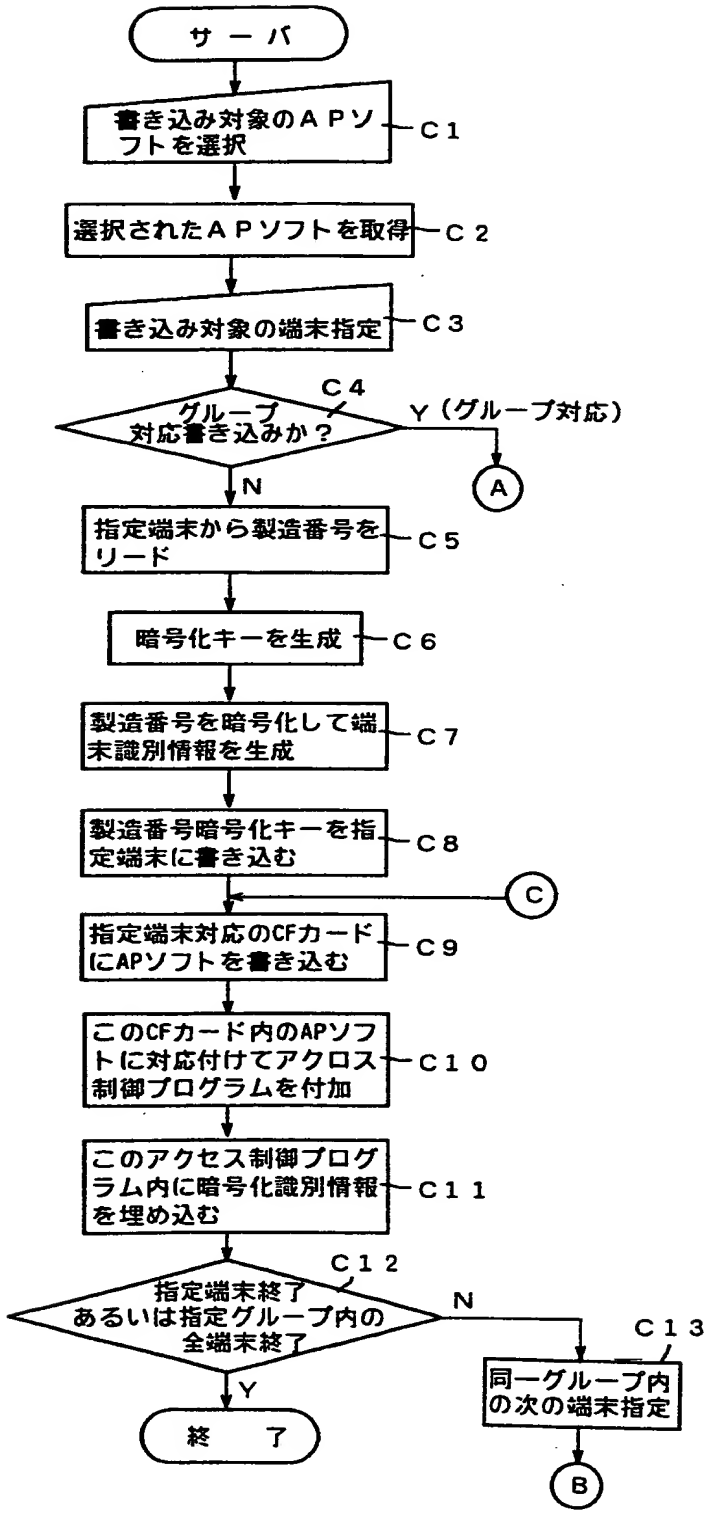
【図６】


A
グループ対応
A１５
グループ内の１台目の端末か？
N
Y
グループ識別情報を入力
A１６
１台目の端末から製造番号をリード
A１７
グループ固有の識別情報を生成
A１８
暗号化キーを生成
A１９
グループ識別情報をこの暗号化キーを用いて暗号化
A２０
スクランブル処理用の暗号化キーを生成
A２１
B
グループ識別情報とその暗号化キーおよびスクランブル処理用暗号化キーを指定端末に書き込む
A２２
C

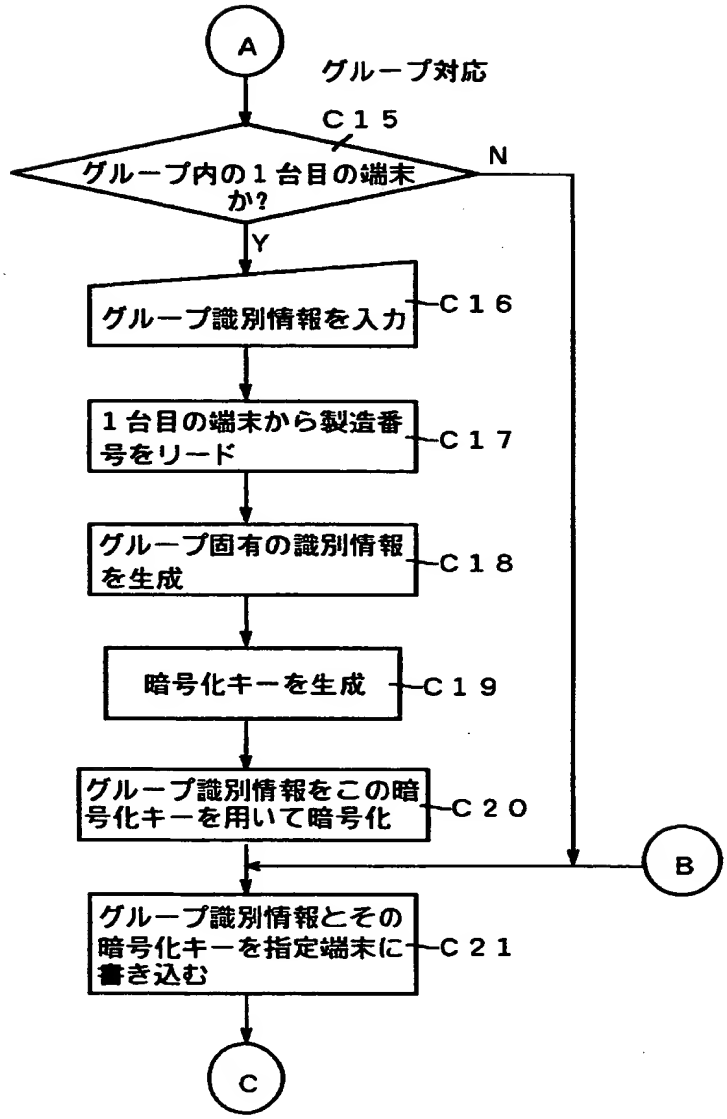
【図７】


端　末
B１
CFカードありか？
N
Y
リターン
CFカードから識別情報をリード
B２
暗号化キーをリード
B３
CFカードからの識別情報を復号化
B４
自己の識別情報をリード
B５
両識別情報の比較
B６
B７
一致か
N
Y
アクセス不可
B８
スクランブルフラグはONか
N
Y
スクランブル処理用暗号化キーをリード
B９
FAT、ルートディレクトリを暗号化キーに基づいて復元化
B１０
アクセス可

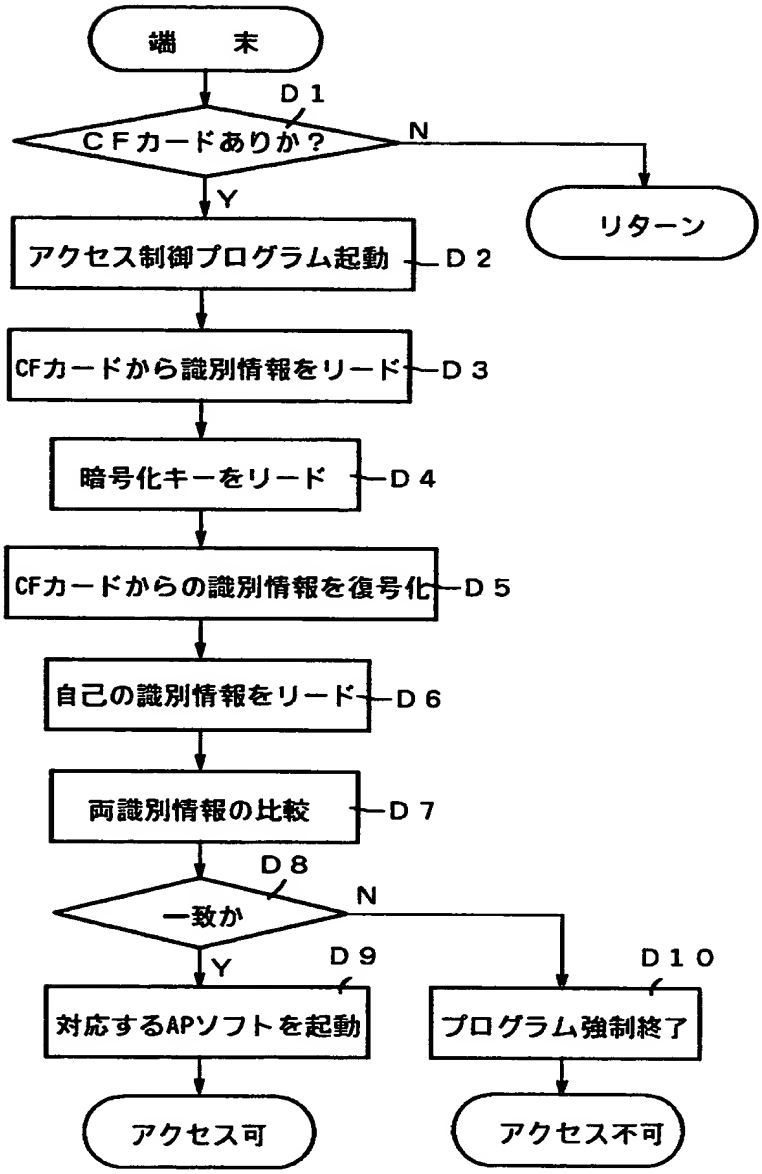
【図８】


サーバ
書き込み対象のＡＰソフトを選択
C1
選択されたＡＰソフトを取得
C2
書き込み対象の端末指定
C3
C4
グループ対応書き込みか？
Y（グループ対応）
A
N
指定端末から製造番号をリード
C5
暗号化キーを生成
C6
製造番号を暗号化して端末識別情報を生成
C7
製造番号暗号化キーを指定端末に書き込む
C8
C
指定端末対応のCFカードにAPソフトを書き込む
C9
このCFカード内のAPソフトに対応付けてアクロス制御プログラムを付加
C10
このアクセス制御プログラム内に暗号化識別情報を埋め込む
C11
C12
指定端末終了あるいは指定グループ内の全端末終了
N
C13
同一グループ内の次の端末指定
B
Y
終　了

【図９】


A
グループ対応
C１５
グループ内の１台目の端末か?
N
Y
グループ識別情報を入力
C１６
１台目の端末から製造番号をリード
C１７
グループ固有の識別情報を生成
C１８
暗号化キーを生成
C１９
グループ識別情報をこの暗号化キーを用いて暗号化
C２０
B
グループ識別情報とその暗号化キーを指定端末に書き込む
C２１
C

【図１０】


端　末
D１
ＣＦカードありか？
N
Y
リターン
アクセス制御プログラム起動
D２
CFカードから識別情報をリード
D３
暗号化キーをリード
D４
CFカードからの識別情報を復号化
D５
自己の識別情報をリード
D６
両識別情報の比較
D７
D８
一致か
N
Y
D９
D１０
対応するAPソフトを起動
プログラム強制終了
アクセス可
アクセス不可

【書類名】　　要約書

【要約】

【課題】サーバ側のアプリケーションソフト／データをＣＦカードを介して端末側に外部提供する場合、カードと端末との対応付けを端末識別情報の一致、不一致およびアプリケーションソフト／データする管理情報の暗号化、複合化によって行うことで、特定の端末に対してのみ、そのアクセスを許可する。

【解決手段】サーバ１は、端末２から端末識別情報を読み込むと共に、読み込んだ端末識別情報の他、ＡＰソフト／データとそのＦＡＴをＣＦカード３に書き込み、カード３内のＦＡＴをクランブル処理して暗号化する。端末２は、カード３内のＡＰソフト／データをアクセスする際に、当該カード３から暗号化された端末識別情報を読み出してそれを復元し、自己の端末識別情報と比較した結果、それらの一致が検出された際に、スクランブル処理されているＡＰソフト／データのＦＡＴ、ルートディレクトリを復元する。

【選択図】　　図1

認定・付加情報

特許出願の番号	平成１１年　特許願　第２６６８５３号
受付番号	５９９００９１６１６８
書類名	特許願
担当官	第七担当上席　　００９６
作成日	平成１１年１０月　７日

＜認定情報・付加情報＞

【提出日】　平成11年 9月21日

次頁無

出　願　人　履　歴　情　報

識別番号　　〔０００００１４４３〕

１．変更年月日　　１９９８年　１月　９日
［変更理由］　住所変更
住　所　　東京都渋谷区本町１丁目６番２号
氏　名　　カシオ計算機株式会社